THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF: **3612 WEST SHAWNEE DRIVE, SPRINGFIELD, GREENE COUNTY, MISSOURI 65810**	**Case No. 22-SW-2083DPR**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Lee Walker, a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

1. I have been employed as a police officer with the City of Springfield, Missouri, since 2004. I am currently a TFO with the FBI, as well as a member of the Southwest Missouri Cyber Crimes Task Force (SMCCTF) in Joplin, Missouri. As a TFO, I have been assigned to investigate computer crimes, including violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended training provided by the Missouri Internet Crimes Against Children (ICAC) Task Force. I have written, executed, and assisted in over 100 search warrants on the state and federal level. As a TFO with the FBI, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have received training in the area of child pornography and child exploitation and have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am authorized by law to request a search warrant.

2. As part of this affiant's duties with FBI, I investigate criminal violations relating to child exploitation and child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents, officers, and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, are currently located at **3612 West Shawnee Drive, Springfield, Greene County, Missouri**, also a location within the Western District of Missouri.

4. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing possession, receipt, distribution, and/or production of child pornography. The property to be searched is described in the following paragraphs and fully in Attachment A. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

5. This affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer, in or affecting interstate commerce, to produce, receive, possess and / or distribute child pornography, are located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, and 2252A, relating to material involving the production, receipt, possession, and/or distribution of child pornography:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), includes actual or simulated: (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to, or operating in conjunction with, such device.

e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other

communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transfer Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

10. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords individuals several different venues for meeting one another, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

13. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Google, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer and/or other electronic devices in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files

or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CELLULAR PHONES AND CHILD PORNOGRAPHY

15. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

16. Cellular phones ("cell phones") are exceptionally widespread. The Central Intelligence Agency estimates that in 2016 there were 416 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images, and the ability to access and browse the Internet.

17. In this affiant's training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

18. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

19. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer-related

documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition,

the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media).

21. Furthermore, because there is probable cause to believe that the computer, its storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF INVESTIGATION

22. During the course of a Crimes Against Children investigation conducted by the FBI - Tampa office, a suspect was discovered possessing a folder containing 13.70 Gigabytes of child sexual abuse materials (CSAM). Accounts of the folder subscriber traced back to **3612 West Shawnee Drive, Springfield, Missouri**, where a registered sex offender named Anthony THURO resides. On or about June 23, 2000, THURO was found guilty of two counts of statutory sodomy in the first degree in the Greene County, Missouri, Circuit Court, in Case No. 31399CF9446. According to the Missouri State Highway Patrol Sex Offender Registry THURO's victims were a 12- to 13-year-old male, and an 8- to 9-year-old female.

23. On or about March 30, 2021, a FBI undercover employee (OCE) was covertly monitoring the Kik group "#livemeusersid." The instructions posted by the chat room bot upon entry to the chat room were, "Welcome! Post on entry LiveMe ID of young girls, you have two minutes. Less active members will be removed. Enjoy the broadcasts . . ."

24. While the OCE was monitoring "#livemeusersid" on March 30, 2021, one of the Kik users in the group sent approximately 40 Mega links to the entire group. One of the distributed links, https://mega.nz.folder/YASXZLC#_AdpLna3B0buNGsRFRbJSQ, resolved to a Mega

folder title "100$" that contained 13.70 Gigabytes of data. Numerous videos of child sexual abuse materials (CSAM) were discovered within the "100$" Mega folder.

25. On January 4, 2022, this affiant reviewed the files and documentation provided to him by FBI Special Agent Michelle Gonzales and FBI Analyst Anthony Agovino from the Tampa FBI field office, regarding the OCE's monitoring of "#livemeusersid" on March 30, 2021, which included the contents of the "100$" Mega folder. This affiant confirmed the folder contained CSAM. The following are descriptions for a random sampling of the videos located on the Mega folder:

a. "…1029.3gp" was a 5 minute, 46 second video depicting an approximately 3-year-old girl seated on the lap of an adult male. The male was spreading the girl's legs to expose her vagina as the central focus of the video. The male rubbed her vagina with his fingers. He then reaches below the girl's vagina and removed his erect penis from his pants. He rubbed his penis against her vagina and attempted to penetrate her vagina with his penis. The girl had a look of distress on her face during the attempted penetration. There was no sound for this video. The clip changed to a nude adult male kneeling behind a nude, approximately 5-year-old girl. The girl was bent over with her ankles bound with a black cord. The male attempted to and then successfully penetrated the girl's vagina with his erect penis. There were similar, additional clips within this one file.

b. "…1030.3pg" was a one minute, 13 second video containing multiple clips of an approximately 7-year-old girl. Only her face was visible, and she appeared to be sleeping. In each clip, an erect penis was being masturbated next to her face. The penis ejaculated on the sleeping girl's face. At times, the girl appeared to wake up and the clip abruptly ended. The bed sheets were consistent in many of these clips.

c. "...146.3gp" was a 2 minute, 2 second video of a nude, approximately 9-year-old girl laying on a bed. Her arms were bound together at the wrists with a yellow rope, she was blindfolded, and a dog was licking her vagina. Occasionally, the person operating the camera rubbed what appeared to be a stick of butter on the girl's vagina to encourage the dog to continue licking her. During this video, the girl began to perform oral sex on the penis of the person operating the camera.

26. On April 2, 2021, Mega furnished subscriber information associated with the "100$" folder, which included multiple Internet Protocol (IP) addresses used to access the folder. These IP addresses were serviced by either Mediacom Communications Corporation or Verizon Wireless.

27. On June 28, 2021, Mediacom Communications Corporation furnished subscriber information for the customer associated with the multiple IP addresses listed in Mega subscriber records. These IP addresses were assigned to Mediacom customer Shannen Malone with a service and billing address of **3612 West Shawnee Drive, Springfield, Missouri**.

28. The FBI – Tampa office obtained an investigative subpoena for the subscriber information for the Verizon IP addresses included in the Mega records. While the Verizon IP addresses that were used to access the Mega folder were non-unique IP addresses, meaning they were assigned to multiple phone numbers at the same time, the phone number (417) 693-7175 frequently appeared in the list of phone numbers that were assigned the Verizon IP addresses used to access the Mega folder.

29. Verizon also included subscriber information for phone number (417) 693-7175, identifying the customer as Shannen Malone, **3612 West Shawnee Drive, Springfield, Missouri**. The customer records listed Anthony THURO as a contact person.

30. This affiant checked the Missouri Sex Offender Registry and found that THURO was a registered sex offender, with a home address of **3612 West Shawnee Drive, Springfield, Greene County, Missouri**. THURO was required to register as a sex offender because of two convictions for statutory sodomy in the first degree. This affiant spoke to Lisa Simmons, the Greene County Sheriff's Office employee in charge of the sex offender registry, who confirmed that THURO reported as required and THURO's information listed on the Missouri Sex Offender Registry was up-to-date and accurate.

31. Springfield, Missouri. Police Department reports, consumer records, Missouri Department of Revenue records, and Greene County Collector records show Shannen Malone-Thuro and Anthony THURO claim **3612 West Shawnee Drive, Springfield, Missouri**, as their residence.

32. This affiant conducted limited surveillance on **3612 West Shawnee Drive** on multiple occasions, and as recently as August 16, 2022. From the public street nearby, this affiant did not find any unsecured WiFi access. I also observed the following vehicles in the driveway of the premise:

a. A black 2014 Nissan Sentra, bearing Missouri license plate RE0D6P;

b. A white 2014 Chevy SUV, bearing Missouri license plate LG2K5S.

According to the Missouri Department of Revenue, both vehicles were registered to Shannen Thuro and Anthony THURO.

PROBABLE CAUSE

33. Based on the above facts, this affiant believes probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime,

or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of 18 U.S.C. §§ 2251, 2252, and 2252A, including, but not limited to, the items listed in Attachment B.

Further Affiant Sayeth Naught.

LEE WALKER
Task Force Officer
Federal Bureau of Investigations

Subscribed and sworn to before me via telephone on the 23rd day of August 2022.

HONORABLE DAVID P. RUSH
Chief United States Magistrate Judge
Western District of Missouri